flow of all necessary command and control information and they define performance and interface requirements for the components of the system. They are intended to document the stated requirements of railroad operational and technical authorities and to influence the design of new, compatible equipment without limiting the internal design approaches of individual suppliers.

To help assess the potential of the ATCS to provide for positive train separation, speed restriction enforcement, and other safety enhancement functions, FRA entered into an inter-agency agreement with the Institute for Telecommunication Sciences (ITS). ITS is the chief research and engineering arm of the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, and serves as a principal Federal resource for assistance in solving telecommunication problems of other Federal agencies, state and local governments, private corporations and associations, and international organizations.

ITS was tasked to study the ATCS specifications and evaluate the system development process, with particular emphasis on the Data Communication System. This technical evaluation of the ATCS will help FRA complete the assessment required by the Rail Safety Enforcement and Review Act. Section 2 provides background material on the ATCS. Section 3 gives general requirements for a collision avoidance system. Section 4 describes the methods used to evaluate telecommunications systems. Section 5 presents the ITS evaluation of the ATCS and Section 6 provides the evaluation conclusions.

2. DESCRIPTION OF THE ADVANCED TRAIN CONTROL SYSTEM

2.1 Purpose and Capabilities of the ATCS

The Advanced Train Control System (ATCS) uses computer-aided techniques to supplement human control in the movement of trains. To accomplish this supplemental role, the ATCS must:

- mimic the current human decision-making steps in the operations of a railroad,
- ensure train movement authorizations are safe, valid, and observed,
- warn railroad personnel of unsafe operations and potential hazards, and
- apply locomotive braking automatically when warranted.

The ATCS imitates the actions of the railroad personnel carrying out railroad operations. As an example, one can compare the steps that occur in originating a train without the ATCS implementation and with the ATCS implementation. In both implementation cases, to originate a train, the dispatcher develops the train route from source to destination, defines the locomotive and car composition, and identifies the crew. The following compares the steps of actions:

- Without the ATCS, the dispatcher uses the voice radio to communicate with the locomotive crew about the train origination. The crew responds with verbal acknowledgements. The dispatcher also passes on information about conditions of the track, locations where track crews would be working, safe train speeds, etc. The locomotive crew copies the information on paper and verbally acknowledges. Finally, the dispatcher provides the authorization for the train movement and the crew acknowledges and proceeds.

- With the ATCS, the dispatcher uses the dispatch data terminal to enter the train origination data into the dispatch center computer. The ATCS checks the information for validity and forwards the information to the on-board locomotive computer. The locomotive crew logs on to the on-board computer through the locomotive terminal to provide crew and locomotive identification, and to confirm the train composition and destination. The locomotive's computer then determines databases required for the planned route and requests them from the dispatch center computer. The dispatch computer supplies the data, including specific track conditions, safe speed limits where track crews are located, and other route-specific information. After the crew has confirmed the train's readiness, the crew enters the message that the train is ready to leave. The dispatcher then requests movement authority from the dispatch computer, which verifies the route is clear of other trains and track crews, that all databases have been received by the locomotive computer, that all restrictions have been received, and that the train is initialized. Track that is not clear is identified for later checks and clearance. The dispatch computer informs the dispatcher of the train's status and the dispatcher then releases the train with its movement authority.

Under the ATCS, all of these steps can be completed without voice communications between the dispatcher and crew. The ATCS ensures that all necessary information is collected and exchanged between the dispatcher and crew. It is also able to provide the information without the ambiguity or misinterpretation that can be associated with voice communications between crew and dispatcher.

The ATCS ensures that actions requested by railroad personnel are safe by checking and verifying the trains' locations and their movement authorizations, by following the track crews' work locations, by comparing locomotive speeds versus safe or restricted conditions, and by validating the proper alignment of switches and other controllable devices, etc. These are steps that would normally be completed by railroad personnel following railroad policy and procedures. The ATCS can perform these steps more reliably and efficiently than humans, thus increasing the likelihood that railroad procedures developed for safety are followed at all times by locomotive crews and track crews.

The ATCS acts to alert and warn the locomotive engineer and dispatcher when unsafe conditions are present. If safe or restricted speed limits are exceeded by the locomotive, the on-board computer warns the engineer to take corrective action. If the computed safe braking distance to the next control point is approaching the safe limits, the engineer is again alerted to begin corrective action. If the dispatcher requests a movement authority of the dispatch computer and the movement is

predicted by the dispatch computer to be unsafe, the dispatcher is alerted of the conflict and the authority is withheld. Again, these are all steps that would normally be followed by railroad personnel; the ATCS acts to supplement the actions of personnel.

Finally, the ATCS intervenes to apply braking for those situations where unsafe operations or hazards exist and the railroad personnel either have not or could not have reacted in time to the warnings.

With the ATCS checking, validating, and (when necessary) overriding the actions of humans charged with following the safe operating procedures of the railroad, the ATCS and railroad personnel can combine their responsibilities to provide for safer train movement. Safer train movement can lead to increased railroad efficiency and greater productivity.

2.2 The ATCS Specifications

The ATCS is a set of specifications developed to provide a unified agreement among the railroads of North America on a train movement control system. The specifications define the performance and interface requirements for the ATCS software and hardware. The specifications must be common to all railroads in order to provide the desired interoperability and compatibility between railroads.

ARINC Research Corporation (ARINC), with the cooperation of the railroads, developed a set of common operating procedures that can be converted into sequences of commands and associated responses. An example procedure might be the set of information and commands sent from the dispatcher to the locomotive engineer to advance from one control point to another; the responses might include the acknowledgements the crew provides to the dispatcher as the train moves between control points. Another procedure might be the command and response required to change a track switch and verify its position. Agreement on the sequence of commands and responses is needed among the railroads so that a train can operate under ATCS on track belonging to several railroads. The train's on-board computer must recognize the commands of the dispatch center and issue its own requests in the manner and sequence required by the dispatch center.

Each procedure, after conversion to a sequence of commands and responses, must be converted to software instructions. The specifications of the ATCS define the procedures and their sequence of commands and responses without defining the software code itself. Since the software is internal to a particular train computer, compatibility demands only that the computer properly recognizes certain commands and provides certain responses, without being concerned about the details of the internal computer operations.

ARINC, with the cooperation of the railroads and equipment manufacturers, developed requirements for the hardware to implement the procedures and to communicate the instructions between the dispatcher, locomotive crew, and other railroad personnel. The hardware requirements define the functions to be performed by the ATCS components, the interfaces between the hardware components, and the information that must pass between the components via the interfaces. The

design goals and features of the hardware components are left to the ingenuity of the equipment manufacturers. The specifications of the ATCS define the requirements for the hardware such that the equipment of the different manufacturers will be compatible, interoperable, reliable, and functional.

2.3 The ATCS Architecture

The ATCS architecture is composed of five major systems [3]. These include four information processing systems: the Central Dispatch System, the On-Board Locomotive System, the On-Board Work Vehicle System, and the Field System. The fifth major system is the Data Communication System, which interconnects the other four systems. The relationship between the five systems is illustrated in Figure 1.

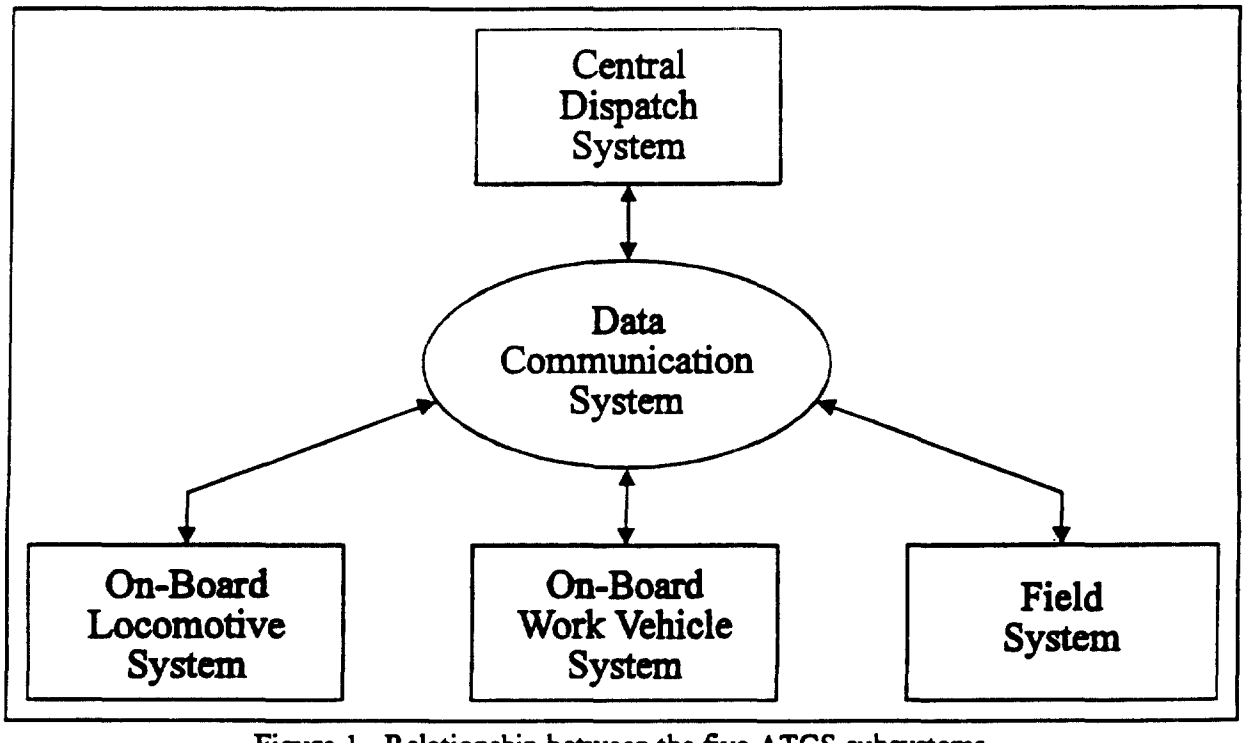

Figure 1. Relationship between the five ATCS subsystems.

These five systems work together to handle requests for information, process data in real time, ensure error-free delivery of data, and handle conflicts and equipment failures. System interconnection is accomplished through a combination of communication nodes and wireline and radio links.

The ATCS Specification 100 on System Architecture explains the functions of the subsystems:

"The function of the dispatch system is to manage the movement of trains throughout the rail network with the objective of guaranteeing safe operations without incurring train delays. The function of the locomotive system is to provide automatic location tracking and reporting, predictive enforcement, and automated transmission of movement authorizations and switch monitoring and control information via the data communication system. The primary function of the work vehicle system is to provide the capability for a track maintenance foreman to communicate with the central dispatch system and other vehicles via the data communication system. The ATCS field system is designed to provide remote monitoring and control of wayside devices." [2]

2.4 The ATCS Levels of Operation

The ATCS is designed for expansion from a basic level of ATCS implementation to a full-capability level. Table 1, also from ATCS Specification 100, provides the capabilities of ATCS at each level, noted as Levels 10, 20, and 30

The ATCS Specification 100 is again quoted to define the levels:

"Level 30 operation assumes that trains are equipped with an enforcement system, a datalink system, an onboard computer, a location system, and a display. Field devices may or may not be ATCS equipped and/or controlled. The dispatcher uses the central dispatch computer (CDC) which can communicate via the datalink to the onboard ATCS equipment and ATCS equipped field devices.

"Level 20 operation is similar to Level 30 operation except that the train has no enforcement capability, no location system, and less sophisticated onboard processing capability.

"Level 10 operation is similar to Level 20 and 30 operation except that the train has no onboard ATCS equipment, or the ATCS equipment on the train is disabled or turned off. Note that in Level 10 no capability exists for the train to contact field devices directly. Also note that field devices are able to function unaware of the equipped level of the train.

"In Level 10 operation the dispatcher delivers Track Condition Notices (TCNs) and Track Work Protection (TWP) to the engineer or foreman via the voice radio. Where railroads have mechanisms in place to deliver written TCNs and TWPs, a confirmation that the items are on hand should be substituted for voice delivery. It is important, however, that the CDC receive verification that the crew has these items in hand. .....". [2]

Table 1. The ATCS Capabilities for Levels 10 through 30

CAPABILITY/LEVEL	10	20	30
Centralized route and block interlocking	R	R	R
Voice delivery of movement authorizations and operating instructions	R	R*	R*
Data delivery of movement authorizations and operating instructions		R	R
Voice reporting of train location to dispatcher	R	R*	R*
Manual reporting of train location and automatic delivery to central dispatch computer		R	R*
Automatic reporting and delivery of train location to central dispatch computer			R
Speed enforcement			R
Movement authorization limit enforcement			R
Monitor and control field devices by code lines from central dispatch computer	O	O	O
Monitor and control field devices by datalink from central dispatch computer	O	O	O
Monitor and control field devices from locomotive cab		O*	O*
Automatic reporting of ATCS device health		R	R
Automatic reporting of locomotive health		O	O

R - Required capability for this level

R* - Required capability to support fallback to lower operating levels

O - Optional capability

O* - Optional capability for field and central dispatch; required on locomotives

2.5 Additional ATCS Design Information and Background

The ATCS is designed according to an international standard called the Open System Interconnection (OSI) reference model [4]. The OSI model serves as a framework for communication architecture and protocol development. It divides the functions that must be performed by a digital communication system into seven layers, with each layer making use of services provided by the layer beneath it. User applications are at the top of the model, while the lowest level is concerned with the transmission of raw bits over some physical medium. ATCS users include dispatch applications, locomotive applications, work vehicle applications, and field system applications. An application is a computer program that processes instructions to satisfy one or more of the operating procedures.

The ATCS data communication system includes several types of nodes [3]. A computer, called the front end processor, is the entry point for the railroad's host computer and dispatch center to the ATCS. The front end processor is connected to several cluster controllers. The function of the cluster controllers is to route data from the dispatch center to locomotives, work vehicles, and field systems. Cluster controllers are normally connected to several base communications packages. These packages provide radio communication to the mobile communications packages of locomotive systems, work vehicle systems, and field systems configured as mobiles.

The communication nodes perform such functions as: vehicle tracking for data packet addressing; data packet routing; data packet flow control; data packet buffering and queuing; data packet prioritization; event timer control; and communication system failure or alarm detection and reporting. These functions are necessary to ensure that data and information are delivered properly and in a timely manner from data senders to data receivers.

The references [2], [3], and [5] provide more detailed descriptions of the ATCS. The details are not repeated in this report, but aspects of the ATCS which are considered important are dealt with in more depth in the following sections.

One of the purposes of the ATCS is to provide safer train operation. The next section defines the concept of collision avoidance from a system perspective and how the ATCS relates to that definition.

3. REQUIREMENTS FOR COLLISION AVOIDANCE

A collision avoidance system provides the means of detecting and preventing impending collisions between vehicles [6]. Such a system performs the following functions:

- Detection of a second vehicle either approaching the planned path or already in the planned path of a first vehicle.
- Evaluation of the collision hazard.

- Determination of the precise maneuver required to avoid a collision.

- Execution of the maneuver.

Positive train separation is the term used within the railroad industry as a synonym for collision avoidance. The ATCS specifications implement a common set of procedures used by the rail industry to provide safe train movement. Consider the following example illustrating railroad procedures for safe train movement and the role of the ATCS in monitoring and enforcing the procedures:

Each train is required to obtain movement authority to advance into a block of track. Inside a block, a train is allowed to proceed to the control point at the end of the block. The ATCS monitors the location of the ATCS-equipped locomotive and its speed within the block. The ATCS computes the required stopping distance of the train as it approaches the control point. If the ATCS determines the conditions are such that the train needs to reduce its velocity or begin braking to stop ahead of the control point, the ATCS alerts the dispatcher and warns the engineer to take corrective action. If action is not taken, the ATCS can enforce corrective action through automatic brake application. The ATCS protects an ATCS-equipped train from a follow-up accident with a slower moving train in the next block. (A "follow-up accident" occurs when a slowly moving train in overtaken by a faster moving train on the same track.)

For ATCS-equipped locomotives operating on ATCS-equipped track, the ATCS can provide positive train separation.

4. EVALUATION OF A TELECOMMUNICATION SYSTEM

ITS has been tasked to evaluate the ATCS as a telecommunication system. Several evaluation methods are available, and two of them are described below. The method selected for the evaluation of the ATCS was one that fell within funding and time constraints.

One method of evaluating a telecommunication system involves modeling, simulation, and testing. Engineers develop software models of the components of the system, combine the software models to simulate the proposed system configuration, and then exercise the combined models by introducing average and peak traffic conditions. Such simulations help to determine the capacity of the proposed system, when and where congestion of the system occurs, and overall system performance. Modeling and simulation provide insight into design decisions prior to committing to building the system, and allow redesign if the simulation indicates weakness.

After the system design is completed but before it is committed to full field deployment, the system is further evaluated by placing it in a working environment on a limited scale. The environment might be simulated initially using hardware in a laboratory, but eventually the system is fully tested under actual field conditions on a test bed where system performance can be monitored.

This method of system evaluation can be completed either by the system designers or by an independent system evaluator. An independent evaluator has the advantage of a certain level of objectivity. The method is thorough, but costly and time-consuming, and because of the limited funds and time available, ITS was not able to perform this type of evaluation and instead used a second approach.

A second method of evaluating a telecommunication system is to review and rate the engineering decisions made in the development process. By reviewing system documentation and discussing particular concerns with system designers, evaluators can make judgments of the engineering choices and overall system design. A useful tool in this type of evaluation is a matrix that identifies key issues that should be addressed in the system development process. The matrix serves as a checklist to guide the evaluators. This is the method adopted by ITS to evaluate the ATCS, and the matrix used is described below.

4.1 ATCS Evaluation Matrix

The matrix used by ITS to evaluate the ATCS has seven columns corresponding to seven general areas of concern that should be addressed in the system development process. Within each area, several elements critical to successful system development are identified. The matrix is shown in Table 2, and the seven areas of concern are briefly described below. They are explored in more detail in Section 5.

Table 2. ATCS Evaluation Matrix

Architecture	Data Communication	Radio Network	Wireline Network	Test and Validation	Migration	Management
Standards-Based	Error Detection and Error Correction	Redundancy	Redundancy	Data Communication Simulation	Implementation and Replacement Plans	Conflict Resolution
Open System	Timers	Radio Frequency Interference	Capacity	Radio Communication Simulation	Continuous Protection During Migration	Hand-off Between Nodes
Common Air Interface	Flow Control and Congestion Management	Signal Coverage		Field Test - Range of Environments		Protection From Threats
Fail Safe	Routing	Blocking and Capacity				
Upgradable Design	Priority					

Architecture defines the structure of the system and the relationship between system components. Evaluation concerns in this area include the process used to determine user needs, whether the design approach was open or proprietary, and whether the system provides for growth and migration.

Data Communication refers to the control of data as it moves from sender to receiver. Concerns include detection and correction of errors that may be introduced along the transmission path, management of data traffic, and priority schemes to ensure that the most important data arrives first at the receiver.

Radio Network and **Wireline Network** refer to the two portions of the data transmission path. Most of the data for the ATCS will be delivered to or received from mobile units. At some point in the transmission path from sender to receiver, data will be sent by means of radio. The remainder of the path will be over fixed wireline circuits. The radio portion of the path operates under constraints that are not encountered on the wireline path.

Test and Validation refer to the means used to test the system to verify that it meets requirements and provides the desired performance.

Migration refers to how the transition from the old system to the new system will take place and what timetable will govern the process.

Management refers to the different methods that system configuration and security are controlled. Concerns include resolution of address conflicts, administrative control as mobile units move through the system, and protection from attempts to corrupt system integrity.

5. EVALUATION OF THE ADVANCED TRAIN CONTROL SYSTEM

Comparing the development of the ATCS against the evaluation matrix leads to a judgment of the soundness of the system design and whether the system can be expected to work as proposed. All design decisions are not reviewed, and a positive evaluation does not guarantee that the ATCS will perform exactly as intended. If, however, the ATCS development process successfully addresses all the evaluation matrix elements, the system is likely to meet its goal of moving trains safely.

The remainder of this section provides a brief tutorial description of each matrix element, followed by an assessment of how well the ATCS development process has addressed the element.

5.1 Architecture

5.1.1 Standards-Based System Development

System designers, software developers, equipment vendors, and system users require interoperability among the components of large data systems. System designers must incorporate standards in the development process to ensure interoperability and compatibility of the system components. The system developers can use existing industry or national standards; in addition, new standards that are specific to the application can be developed and used by the system designers.

A railroad industry committee acted to develop the ATCS based upon railroad needs, equipment vendor capabilities, and proven data communication techniques [3]. With time, the committee has evolved the specifications based upon knowledge gained from the railroads and manufacturers as the specifications are tested for desired results, required performance, and possible implementation. As a result, the specifications have become a standard, in the usual sense. If all manufacturers, system integrators, and railroads adhere to the specifications, then the resulting train control systems of the railroads will be interoperable and compatible.

Matrix Element Evaluation *The ATCS specifications define performance and interface requirements for the hardware and software components of the system. This use of a standard is necessary to ensure that those system components and operations that affect train safety are defined the same way throughout the entire system, across all railroad systems.*

5.1.2 Open System

The need for dissimilar data systems to communicate with each other has led system designers to establish both physical and protocol standards for linking different data system equipment together. The equipment of different manufacturers must be able to interface to each other physically. This is accomplished by setting hardware standards. Likewise, the information passed between the different manufacturers must be of a format that each piece of equipment understands. These standards for communications between computers and data systems have developed on an international level with the International Standards Organization fostering a reference model for Open Systems Interconnection (OSI) [4]. The OSI model consists of a seven-layer communications architecture with each layer having its own set of protocol or rules for communications. Several advantages of an OSI structure are:

- all vendors have an opportunity to supply equipment to meet the users' needs,
- different equipment from different vendors (or even the same vendor) will be designed for interoperability,

- different data communications design groups can work on specific layers independently of other groups assigned to other layers, and

- as technology changes, the affected layer's protocols can be modified without affecting the other layers.

The ATCS endorses the reference model of OSI. Specifications are written with an open system approach and follow the OSI guidelines.

Matrix Element Evaluation *The use of the OSI model for systems development will benefit the railroads and the vendors. The greatest benefit is that the OSI philosophy allows the incorporation of new technology as it becomes available and is needed by the railroads. As new devices or technologies are developed that assist in positive train separation, the ATCS will have the framework that allows their introduction in the easiest possible way.*

5.1.3 Common Air Interface

Much like the Open System Interconnection model between computer and data systems, the Common Air Interface concept has been developed for the radio portions of communications networks. A Common Air Interface is a standard that ensures that the radio equipment will be interoperable with radio equipment from different manufacturers and compatible with radio systems for different users (railroads). Such an interface standard disallows the use of media access schemes, modulation techniques, or any other radio air interface specifications that are considered proprietary, unless all vendors are allowed to use the proprietary techniques in the design of all radios for the application. In an approach such as the Common Air Interface, new techniques, designs, and solutions are encouraged to counter difficulties in radio communications, but the resulting intellectual properties become available to all competitors and users of the system.

The ATCS specifications indicate the characteristics for digital communications by specifying the radio channel bandwidth, radio channel bit rate, modulation, channel access, and frame formats including codes for error detection and correction [5], [7]. No proprietary measures were indicated in the specifications, allowing for a common air interface.

One possible potential for the growth of the ATCS is to consider the voice and data radio system currently being developed by the Association of Public-Safety Communications Officials, the National Association of State Telecommunications Directors, and the Federal Government [8]. Their standard for digital land mobile radio incorporating both data and voice is known as the APCO-25 Standard. Consideration of the Standard could result in a cost savings for railroads and allow compatibility with other users in the band.

Matrix Element Evaluation *The air interface is defined for the ATCS and allows for compatibility between various vendors' systems and between various railroads. Compatibility of the radio systems will be required to serve rail safety to the maximum possible extent.*

5.1.4 Fail Safe

Fail Safe is defined as a specific quality of a system such that the system continues to function (with reduced performance) after the failure of some component or piece of the system [6]. For example, a traffic light control malfunctions and the light begins to flash red in all directions, indicating traffic control is being returned to the individual drivers of the cars entering the intersection. This system performance change, without a complete system shut-down due to a system failure, is considered to be fail safe. In some of the ATCS documentation, the term fail passive is used, as "that property of a system to recognize that a failure has occurred and transition into a passive state to avoid adverse affects on system operation." [9]

The purpose of our examination is to examine the data communications systems of the ATCS as they relate to collision avoidance. From this perspective we can modify the initial definition to say, a fail safe architecture is one that continues to provide collision avoidance after the failure of some component or piece of the system. In the case of an automated control system, the desired actions usually are:

- identify the failure(s),
- notify the human managers of the problem, and
- defer all decisions to the human manager until the problem is corrected.

The ATCS Specification 200 states that the elements of the ATCS required to ensure safe train movements and track occupancies are considered Vital Elements. Vital Elements of ATCS are those related to the organization, issuance, safe execution, and enforcement of movement authorities. If the failure of a vital element occurs, the system must fail in a safe failure mode, selected to eliminate hazardous consequences

Matrix Element Evaluation *The ATCS design acknowledges that vital components will fail. As with other control systems developed for fail-safe shut-down operations, the ATCS is designed to shut down safely and to relinquish decision-making responsibilities to the human operators, the dispatcher and locomotive engineers.*

5.1.5 Upgradable Design

A goal of system design today is to avoid locking the system into current technology. Systems need to be able to incorporate new technologies as they become available and are needed by the users. Open, standards-based systems have the best opportunity to expand with new technologies and applications. Designers and manufacturers are more likely to provide technological improvements to systems which have well-defined, non-proprietary interfaces than those which do not.

As discussed above, the ATCS has been developed with upgrading as a potential migration path. One area where expansion is already allowed is that of negotiating between a cluster controller (CC) and a mobile communication package (MCP) on a locomotive or track maintenance vehicle that has come into the controller's area. The negotiation allows the CC and MCP to decide which protocols they both understand and what are the associated parameters. This form of negotiation allows the system to expand, allowing new protocols to be established with newer equipment, but retain the capability to communicate with older equipment supporting older protocols.

Matrix Element Evaluation *A system that allows expansion from its present configuration and operation will serve the interests of railroad safety. New application programs can be developed to further ensure positive train separation, even with tighter spacing between trains. The application programs can utilize newer techniques, developed in other industries, to solve the problems faced by the railroad industry. Techniques such as Kalman Filters [19] and Fuzzy Logic [20] use information from the process they are trying to control to improve the process in a real-time, adaptive manner. The ATCS has the framework to allow the software and hardware to migrate and expand in performance.*

5.2 Data Communications

5.2.1 Error Detection / Error Correction

Transmission errors occur in all data communication systems. While today's technologies and transmission media have dramatically reduced the frequency of errors, errors can never be totally eliminated. A properly designed system must have the ability to detect and handle errors in their transmitted data.

There are two basic strategies for dealing with data transmission errors. The first strategy is to detect errors and request a retransmission of the data packet containing the error. The second strategy is to correct the detected error at the receiver.

An error-detection-only strategy includes, with each data packet transmitted, a code called a cyclic redundancy check (CRC) that allows the receiver to determine the presence of an error in a given block of data. The receiver may then request that the flawed data packet be retransmitted. The process is repeated until the receiver accepts a flawless packet. This method is called automatic

repeat request (ARQ), because if an error is detected the receiver automatically requests that the packet be repeated (retransmitted). This strategy has the potential problem of requiring the data system to provide a large number of retransmissions as the result of isolated, single-bit errors.

An error-correction strategy places enough overhead into the data packet to allow the receiver to detect and correct most errors, if they are of the isolated, single-bit variety. The amount of data redundancy, in each data block, needed to detect and correct errors is greater than the amount required for simple error detection; however, the total amount of data passed from sender to receiver may be reduced with an error correction scheme if errors occur often enough to cause frequent retransmissions in a detection-only scheme. Error correction is frequently called forward error correction (FEC) because the receiver corrects the errors. When these two strategies are used together, the technique is called modified ARQ.

The ATCS uses modified ARQ for two reasons. The ATCS system designers examined several received data files that had been transmitted over typical railroad radio channels [7]. The errors that occurred in the data indicated in most cases errors would be present as isolated errors in a data block. An FEC scheme is ideal for correcting isolated errors. The other cases of errors in the data indicated a large number of errors occurred together, in a burst. Error bursts are best dealt with by a retransmission of the data block. FEC corrects isolated errors without requiring large numbers of retransmission. The FEC capability allows the system to recover from small errors without excessively large amounts of overhead. The ATCS uses a type of FEC called Reed-Soloman, after the code's designers. This error correction method uses 25 percent overhead (20 of 80 bits) to identify and correct errors occurring in a group of two or fewer five-bit symbols in error per block. The method was chosen after examining five different FEC correction methods. All these methods were tested against four different channel error files. The Reed-Soloman method of FEC was selected because of its throughput and its relatively high performance on all tests which were conducted.

Matrix Element Evaluation *The decision process used by ARINC and the Component Specification Drafting Committee (CSDC) follows a logical progression. The committee and ARINC determined that the most likely errors within a data packet would be isolated in occurrence and could be corrected by FEC without introducing large amounts of overhead into the system and that a Reed-Soloman code was best for their needs. The decision to use ARQ to recover from bursts of errors within a data packet was retained because it mitigates the need for large amounts of error correcting overhead.*

5.2.2 Timers (Time Outs)

Timers or time outs provide the ability of a system to manage and control the time allotted for different functions. The purpose of these timers might be to control run times for different functions or to measure time periods during which responses are to be received. Timers prevent a system from waiting an inordinate amount of time for the completion of a task, and prevent a system from

retaining information for an unacceptable amount of time. Timers are especially important in a system that must integrate components that are produced by different manufacturers. A system cannot successfully function without the use of timers as part of its flow control/congestion management scheme. The ATCS employs timers in many different functional areas. Examples include the following:

- When a train enters the system (starts up), the cluster controller sends a message to its adjacent cluster controllers informing them about the new train. The adjacent cluster controllers modify their individual address tables to reflect the new entry. If that address is not referenced within a set amount of time, the adjacent cluster controller may purge or erase the idle entry from its table. In this case, a timer is used to manage memory and buffer space.

- Carrier sense multiple access (CSMA) is a method used by the ATCS to allow many radios to share the same radio channel or frequency. If a radio wishes to transmit, it first listens to determine if that channel is busy. If it is busy, the radio "backs off", waits a random amount of time, before trying to transmit again. The ATCS uses an initial "back off" window of 10 - 200 ms. The timer assists in flow control and congestion management. The back-off/delay time constants used in the ATCS radio network were taken from those used by other similar radio networks.

Matrix Element Evaluation *The use of timers is essential to minimize the congestion of the system and to allow different brands of equipment to work together. The ATCS employs timers at important junctures. The settings of these timers is based on sound logic and empirical data. Whether or not the time limits selected in the specifications are the best possible will be determined as the result of system simulation, equipment interoperability tests, and actual field experience. The tests and experience will lead to improved implementation of system timers.*

5.2.3 Flow Control / Congestion Management

Flow control refers to techniques employed to ensure that a data sender does not overwhelm a receiver before the receiver has an opportunity to process incoming data [10]. Because of the layered approach of the OSI model and the various system configurations, flow control may take place at many different OSI layers within a data communication system.

There are several different types of flow control. Two of the most common are stop-and-wait and sliding window. Stop and wait directs the sender to wait for an acknowledgment from the receiver before sending the next packet. Sliding window flow control allows the receiver to accept several packets before sending a group acknowledgment.

Congestion management is the ability of the system to protect itself from "congestion collapse". Congestion collapse occurs when system data buffers overflow and data transmission queues become so long that data throughput ceases.

The ATCS employs several different methods of flow control. The data link protocol used, high level data link control (HDLC), has the capability to provide a "receiver not ready" command. The ATCS also uses a sliding window flow control method. This provides greater utilization of the communications channel than the stop-and-wait flow control method.

As defined in Section 5.1.2 on the OSI Model, the system has seven layers for communications. The ATCS layer 3, the network layer, acts as a control point between the transport and the data link layer. If the network layer receives a congestion message from layer 2, it will control the information it receives from layer 4, discarding traffic starting with that having the lowest priority until the congestion is cleared.

Matrix Element Evaluation *Data flow control and congestion management are required aspects of a well-designed data communications system. The ATCS has been designed with a thorough understanding of flow controls and congestion management, and uses proven techniques to manage a potentially catastrophic problem.*

5.2.4 Routing

Routing can be defined as the method by which a data packet or message is directed from node to node through a data communication system [10]. Many different types of routing are available and may be organized into two categories:

- Non-adaptive routing bases routing decisions on a fixed set of rules that do not change with time.

- Adaptive routing bases routing decisions on updated information of traffic loads and system configuration and attempts to use the "best path".

The routing mechanism selected for a particular system depends largely on needs of users. As a rule, adaptive routing is better suited for situations when stations may move, traffic loads vary, or the configuration changes.

Three different types of algorithms are used for adaptive routing. Global algorithms, the first type, use information from the entire system to make routing decisions. This method can suffer from excessively large and cumbersome routing tables. The second type is a local algorithm which allows each individual node to determine routing. The third type of algorithm combines both global and local methods into what is known as distributed routing

The ATCS uses distributed routing. Each node periodically updates its neighbors about addresses it is able to reach. When there is traffic for that address, the other nodes point the traffic toward the controlling node. In cases where addresses are not known, the global directory is consulted. If this fails, an orderly, expanding search is generated in the attempt to locate the address. The ATCS controls its routing table size by periodically purging unused addresses from the routing tables.

Matrix Element Evaluation *The ATCS uses adaptive distributed routing to transmit data from sender to receiver. As the system is reconfigured due to growth and migration, the system will be able to route the data along the most efficient paths afforded by the new configuration.*

5.2.5 Priority

Priority provides the data sender with a means to designate some messages more important than others, thus expediting their delivery. A priority scheme is extremely important in systems where emergency traffic may be present. It is also an important component of congestion management. High priority traffic is usually allowed to proceed while low priority traffic is discarded during periods of data traffic congestion.

The ATCS uses priority to its fullest advantage. The requirement of four priority levels was derived through many user group meetings. Each message format has an assigned priority level. The priority scheme allows three procedures to be followed:

- Each message format is required to have a preassigned priority thus preventing an application or component from choosing an inappropriate priority for one of its messages.
- The data sender is required to always attempt to send the highest priority messages out of its buffers first.
- Each message is required to be checked for its level of priority before it is delayed or purged during periods of data congestion.

Matrix Element Evaluation *The ATCS priority levels have been developed in a logical manner. A four-level priority scheme was chosen to reflect user needs and operational requirements. Methods for expedited handling of high priority traffic allow the data communication system to be used to its fullest advantage.*

5.3 Radio Network

5.3.1 Redundancy

Redundancy is duplication of elements in a system or installation for the purpose of enhancing the reliability or continuity of operation of the system or installation [6]. Redundancy can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.

Redundancy, as related to radio communications, is defined as the availability of duplicate radio transmission and reception means to support the system in the presence of failures in the primary system [6]. The examination of redundancy is important because it relates to the system's ability to continue to function despite failures.

According to the ATCS design rules, a duplicate ATCS data radio system to provide backup support to the primary ATCS data radio system is not a requirement. In case of failure of the ATCS data radio system, the voice radio system is to provide the fallback operation in the ATCS (see Table 1 which provides the ATCS capabilities for Levels 10 through 30). Table 1 indicates, at Level 30, that speed enforcement and movement authority limit enforcement are still available in the event data radio communications have failed, even though the ATCS must rely on voice delivery of movement authorities and operating instructions, and voice or manual reporting of train location. In this situation, redundancy is accomplished by the use of functional diversity; the independent voice radio communication system is used to replace the data radio communication system.

Both technology and policy of voice radio communication systems, as used by the railroads and other land mobile radio users, are undergoing changes. Technology is moving towards digitizing voice for voice radio communication system applications. Policy changes will modify the equipment characteristics as well as require the systems to be more efficient and support greater user capacity. As the ATCS matures and as the changes to the railroads' voice radio communication system are implemented, the ATCS could rely on the voice radio systems as a redundant system providing digital data communications. If voice is digitized for transmission and reception on a digital voice communication system, then any digital signal may be handled by the voice radio communication system as well.

Matrix Element Evaluation *Redundancy of the ATCS data radio system is not accomplished through duplicate equipment to automatically replace failed equipment. Instead, the ATCS falls back to the voice radio system to provide the movement authority and location information. The railroads' design rule as a response to the failure of the ATCS data radio communication system is not unlike present procedures used when the voice radio system fails. The procedure requires the locomotive engineer to observe safety rules and advance the train to the next location providing telephone service for communications with the dispatcher.*

5.3.2 Radio Frequency Interference

When designing a radio communication system, the designer must consider not only what capabilities the system must have, but also the radio environment in which the system must operate. Radio systems are vulnerable to unwanted disturbances, superposed upon a useful signal, that tend to obscure the desired signal's information content [6]. Disturbances produced by other transmitters within the frequency band of the desired system are generally referred to as interference, while broadband disturbances across a wide range of frequencies whose sources are man-made (such as arc welders), atmospheric, or internal to the radio system itself are referred to as noise. System designers must take steps to protect a radio communication system from interference and noise.

The ATCS development included studies to measure or analyze the interference and noise environments of the ATCS [11]. A measurement study consisted of a comprehensive interference and noise examination of the locomotive's cab. This was done to establish a reference interference and noise environment due to the internal locomotive components. The ATCS components must be designed to accommodate the measured reference levels.

The second significant study was an environmental analysis of the radio communication channel's operating environment [12]. The ATCS must operate in radio-congested cities as well as across vast plains. Interference from other radio services is a major concern in most metropolitan areas. Of the two frequency bands considered, Very High Frequency (VHF) and Ultra High Frequency (UHF), the UHF band presently experiences less radio congestion in metropolitan areas.

Matrix Element Evaluation *ARINC examined the implications of noise and interference on the frequency bands selected for the ATCS. The first examination evaluated the electromagnetic environment of the locomotive and provides guidance on the radio environment to the equipment designers. The second analysis identified the UHF band as the more desirable of the VHF and UHF bands in metropolitan areas.*

5.3.3 Signal Coverage

Signal coverage is the condition whereby a base station and mobile have reliable communication service for a specified percentage of time, typically 90%. The signal coverage area is the area surrounding a base station that meets the conditions for signal coverage. A line that can be drawn around the coverage area, such that the enclosed area meets the signal coverage conditions is called the coverage contour, for example the 90% coverage contour [6]. Communications outside the contour can occur but not with the desired 90 percent reliability.

Several factors influence signal coverage. Terrain, vegetation, and man-made obstacles between transmitter and receiver influence the received signal's amplitude and structure. Radio communication system designers need to know typical conditions for the radio system to plan its design. Noise and interference are other factors that can reduce signal coverage. Typically in rural environments, radio

coverage is limited by weak desired signals, whereas in urban environments, coverage is limited by the presence of interference from undesired signals.

There were two different frequency bands under consideration, VHF (160 MHz) and UHF (900 MHz). These frequencies have distinctly different propagation or coverage characteristics. As frequency increases, the propagation loss also increases. Thus to deliver the same power to a radio receiver at UHF as at VHF, the UHF transmitter must have a greater radiated power level compared to the VHF transmitter. For this reason, VHF is preferred over UHF for long distance communications, in rural and mountainous areas.

As frequency increases, atmospheric and man-made noise decreases. The band selection would then favor UHF. A principle consideration in selecting UHF was its performance in cities and the relative uncluttered spectrum as compared to VHF. A study conducted by Battelle provides support to the decision to use UHF. UHF is a weaker choice than VHF in open terrain and through foliage. Battelle points out that by increasing antenna height, increasing transmitted power, or increasing the number of base stations, some of the disadvantages of UHF versus VHF may be reduced. [12]

Signal coverage performance models provide guidance on required spacing and location of base stations along track routes to provide the desired signal coverage [12-14]. In practice, exact base station location or characteristics can be adjusted to fill in areas which have experienced poor coverage.

Matrix Element Evaluation *The railroads presently use assigned spectrum in the VHF band for voice communications. The FCC has made additional spectrum available to the railroads in the UHF band to be used for data communications. Presently, the allocated UHF spectrum has less noise and interference than does the allocated VHF spectrum. The disadvantages of UHF signal coverage compared to those of VHF can be overcome by good base station site selection.*

5.3.4 Blocking and Capacity

Blocking occurs when one user wants to use a radio channel already in use by another user. The second user must wait until the channel is not busy before sending any radio traffic. Severe blocking occurs when more users are waiting with messages to send than can be handled within the specified time limits for message delivery.

Two concerns follow from the issue of blocking. The first concern is whether there is a means to recover from the congested state. This concern was covered under flow control and congestion management. The second concern is whether there is sufficient capacity to handle the amount of traffic that the ATCS might typically be expected to handle. This is particularly important with the ATCS radio system which uses a CSMA scheme (see Section 5.2.2).

Automated Monitoring and Control International (AMCI) has studied the issue of blocking and capacity of the radio channel [16, 17]. The studies evaluated the ATCS channel as specified in Specification 200, analyzing work order reporting for a national, twenty train system with position location. The data used in the studies represented operating radio traffic from the Union Pacific Railroad. The reports conclude, based upon work order reporting, that no problem with congestion exists.

A need for increased capacity may become necessary as the railroads provide more information to be communicated via the ATCS. As with the cellular-phone industry, the railroads may have to add more base stations to handle increasing capacity due to more data traffic between mobiles and base stations. The additional base stations would operate with reduced power characteristics but would increase the density of the stations along the route. Since each base station can handle a certain average number of messages (trains), increasing the number of base stations along a track segment will increase the total number of trains that can be accommodated.

Matrix Element Evaluation *Congestion and blocking of the radio channel are significant concerns. While the ability exists to clear the channel if it becomes blocked, the ideal method is to avoid blocking through sufficient capacity. The studies conducted by AMCI address the capacity concerns. The studies only model work order reporting traffic. The Chicago hub, with its concentration of locomotives, provides an example of a severe communications environment. A more thorough understanding of the data traffic levels, in typical as well as severe communications environments, needs to be developed and modeled to ensure that the system has been properly designed for all potential geographic areas.*

5.4 Wireline Network

The wireline network is defined here to include all equipment of the ATCS other than that directly used for radio communications. Thus the wireline network includes components such as the dispatch computers, front-end processors, cluster controllers, way-side devices, field equipment, and the land line connections between computers, controllers, field equipment, etc.

5.4.1 Redundancy

For a definition of redundancy, see Sec. 5.3.1.

Critical, vital computer systems are designed with redundant modules operating side-by-side, with the ability to immediately detect and alert both other system equipment and system personnel when there has been a failure in either computer. While one side of the redundant computer system awaits repairs, the other carries out its tasks. Thus they have high levels of availability, and low error rates.

Front-end processors and cluster controllers, for example, are not designed with redundant components operating side-by-side. Instead, the connections between front-end processors and

cluster controllers are made in a mesh configuration. In other words, there are primary connections between a front-end processor and its cluster controllers. There are also connections from the processors to cluster controllers served primarily by other processors. In the event a processor or controller fails, other equivalent devices can be commanded to service the failed unit's clients until the unit is repaired or replaced. Similar connections are made between cluster controllers and the equipment such as base stations that the controllers serve.

System designers have a tradeoff option between the design of a component that has a very long time between component failures and a design that uses two relatively inferior components in a parallel or redundant operation. To understand the difference between redundant operation and a high mean time between failure (MTBF) design, consider the need to have a light on in the locomotive cab. The designer could have put two light bulbs operating in parallel (on simultaneously) or the designer could have used a single light bulb. Suppose in the case of the two light bulbs, the MTBF is 200 hours for each bulb. The equivalent single bulb would require a MTBF of 1600 hours to provide the same performance.

A report by Draper Laboratory provided the ATCS development team with an analysis of the relative contribution of the various ATCS elements to the overall accident rate under ATCS Level 30 operation. The report identifies those elements required to have redundant (or dual) operation and those required to have high MTBF designs [18]. The ATCS has been developed with those requirements as factors.

Matrix Element Evaluation *An engineering organization modeled and developed the requirements for availability and these requirements were incorporated into the specifications. Vital components, as defined by the railroads, are required to be designed using redundant modules. Other components use multiple connections between like equipments to support redundancy features. Redundancy in the wireline network of the ATCS is required to support safety. In some cases, redundancy is provided functionally, where failure of some components forces the ATCS to fall back to reliance on voice communications, for example.*

5.4.2 Capacity

Capacity refers to the ability of a system or component to handle a certain or predetermined level of traffic. For components such as the dispatch computer, capacity might be described in instructions per second. For wireline connections such as the link between cluster controllers, capacity might be described in bits per second.

The ATCS does not specify requirements for absolute capacity since that would vary with the number of trains being served. Instead, Specification 200 provides requirements for maximum acceptable delay. A specification that mandates a maximum packet delay time ensures that the different priorities of traffic receive appropriate handling. By establishing a delay criteria as opposed to a throughput

capacity, the ATCS specifications are more realistic and the system is more able to efficiently handle different degrees of message priorities throughout the network.

Matrix Element Evaluation *By establishing data delay criteria, the ATCS states the requirement for the data communication system. Component manufacturers and system integrators have the freedom to provide the necessary capacity in different ways to satisfy the data delay requirements.*

5.5 Test and Validation

5.5.1 Data Communication Simulation

Simulation is the creation and use of a model that behaves or operates like a given system when provided a set of controlled inputs [6]. Simulation is used in place of a system (under development, for example) to verify expected performance, to test responses to various stressful conditions, and to validate operational sequences. Simulation can be composed of software models, hardware models, or a combination of both. Using simulation techniques, conditions can be changed in a step-wise process to determine when and why a proposed or functioning system breaks down. A simulation can model a proposed modification to the system and can be used to evaluate the modifications using the exact conditions that were applied earlier to stress the system.

Simulation and modeling are required early in the development effort, prior to implementation. Field testing of prototype systems is also required, but field testing rarely allows the testers to repeat conditions exactly or apply extreme situations that the system may eventually encounter. In addition, deficiencies uncovered during simulations are usually corrected with much less expense than those uncovered during field testing.

The need to model data communications has been established for the ATCS. Modeling of data communications accomplishes two tasks. First, it ensures the different communication layers interact as expected and do not develop bottle necks. Second, it allows validation of different vendors' implementation of protocols. Currently, AAR has contracted for a simulation tester to test lower layers of data communications equipment. Recent conversations indicate this will be modified to test all layers.

Control flow specifications provide functional descriptions of certain aspects of railroad operating logic, and define how hardware and software elements of the system should interact in order to execute railroad operations. The ATCS execution of railroad operations is through applications, which are computer programs that are processing instructions to satisfy one or more of the operating procedures. Each time a dispatcher or an application generates a command, control, or information message to be delivered to a locomotive or signal, a series of events occur that are related to the message generation. Control flows are extremely complex because of the logic necessary to translate railroad procedures into events that are to be carried out by the ATCS, and because of the validation that must precede and follow-up the occurrence of each event. For example, one of the ATCS

control flows describes the process by which central dispatch would issue a movement authority to a locomotive, and defines the associated messages that would be exchanged between various system processors. Correct control flow is necessary because safety can be affected by improper logic allowing a wrong translation of railroad procedures into events to be performed by the ATCS or by a wrong sequence of events to be followed by the ATCS. As an example, if control flows allow a locomotive to continue on after an unexpected transponder address is read, then those control flows may not be able to detect the potential for a collision.

A major revision of the Control Flow Specifications was completed in 1993. The control flows have become increasingly complex as system development has progressed. ARINC is working on further documentation to aid ATCS software developers.

The control flows are sufficiently important to warrant further study of the development effort. For example, individuals who write control flows should not be asked to validate them. An independent validation of the control flows or an independent simulation of the control flows should be completed. The Draper Laboratory report also noted "the exhaustive technical analysis of the ATCS system logic and the development of engineering tools to control the implementation of the system logic will serve to reduce the risk of this as an accident cause." [18]

Matrix Element Evaluation *The ATCS is a complex system that requires numerous different entities to interoperate in a dynamic situation. Simulation is a method used to assist system developers evaluate whether system components are interoperating as desired. Hardware emulation efforts are currently underway to evaluate vendor products in their compliance with the data communication specifications.*

Because of the complexity of the control flows and because correct control flows are essential to safety, ITS recommends independent modeling and validation of the ATCS control flows under a variety of operating scenarios to ensure that the system functions as intended.

5.5.2 Radio Communication Simulation

Radio communication simulation is similar in purpose to data communication simulation as described above. The radio simulation efforts are somewhat different as the radio environment and communications channel must be modeled. The radio environment simulation involves modeling of radio interference and noise. The communications channel involves modeling of varying signal levels due to the propagation conditions caused by foliage, rugged terrain, tunnels, etc., and the modeling of varying self-interference at the receiver due to multiple reflections of the transmitted signal along the path between transmitter and receiver (i.e., multipath).

Battelle has analyzed the radio environment to compare the VHF band performance with UHF [12]. Both AMCI and Rockwell have laboratory equipment to simulate the radio environment and channel.